Please enter the following new Claim 15:

Rule 1.126

B1

~~15.~~ 16. (new)

A system of co-operating computer entities including:

a first computing entity comprising::

a data processing equipment

a memory; and

a communications equipment,

said data processing equipment being configured so as to be capable of processing data according to a set of instructions stored in said memory;

said communications equipment configured so as to communicate data according to said set of instructions such that the computing entity is configured to

a) receive from another computing entity a number P such that P is a prime number and $n|(P-1)$;

b) provide to said other computing entity a number g where $g = f^{(P-1)/n} \bmod P$, $f< P$;

c) receive from said other computing entity numbers A and B, where $A = g^p \bmod P$ and $B = g^q \bmod P$;

d) check that $A \neq B$, $A \neq 1$ and $B \neq 1$, and, if correct, repeat up to k times;

e) select a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$ and

provide the number h to said other computing entity;

f) receive from said other computing entity $U = g^{2u}$, $V = g^{2v}, H_U = B^{(h^u \bmod n)}$, $H_V = A^{(h^v \bmod n)}$, and $H_{UV} = h^u h^v \bmod n$ entity were u and v are two random numbers such that $\ell(u) = \ell((p-1)/2)$, $\ell(v) = \ell((q-1)/2$;

B1 cont

g) request the other computing entity to provide values r and s, randomly specified to be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p - 1)/2$, $s = v + (q - 1)/2$;

h) receive the requested values r and s from the other computing entity,

i) if $r = u$ and $s = v$ was requested, determine whether:

(1) $\ell(r) \le \lfloor \ell(n)/2 \rfloor + d$, $\ell(s) \le \lfloor \ell(n)/2 \rfloor + d$,

(2) $g^{2r+1} \equiv Ug$, $g^{2s+1} \equiv Vg$,

(3) $B^{(h^r \bmod n)} \equiv H_U, A^{(h^s \bmod n)} \equiv H_V$,

and

(4) $h^r h^s \equiv H_{UV} (mod\ n)$;

thereby verifying the values provided by the other computing entity are as were required by steps a) to i); or, if $r = u + (p - 1)/2$, $s = v + (q - 1)/2$ was requested, determine whether:

(1) $\ell(r) \le \lfloor \ell(\mathrm{n})/2 \rfloor + d,\ \ \ell(s) \le \lfloor \ell(n)/2 \rfloor + d,$

(2) $g^{2r+1} \equiv UA,\ g^{2s+1} \equiv VB,$

B1 con't

(3) $B^{(h^r \bmod n)} \equiv H_U^{\pm 1}, A^{(h^s \bmod n)} \equiv H_V^{\mp 1}$ *(± and ∓* meaning the two exponents are of opposite sign), and

(4) $h^r h^s \equiv H_{UV}\ h^{(n-1)/2}\ (mod\ \mathrm{n});$

thereby obtaining said probablistic evidence on whether the given public-key number n is the product of exactly two odd primes p and q whose bit lengths ($\ell(p)$, $\ell(q)$) differ by not more than d bits; and

a second computing entity comprising:

a data processing equipment

a memory; and

a communications equipment,

said data processing equipment being configured as to be capable of processing

data according to a set of instructions stored in said memory;

said communications equipment configured so as to communicate data according to said

set of

instructions such that the computing entity is configured to:

a) provide to another computing entity a number P such that P is a prime number and $n \mid (P-1)$;

b) receive from the other computing entity a number g where $g = f^{(P-1)/n} \bmod P$, $f < P$;

c) provide to said other computing entity numbers A and B, where $A = g^p \bmod P$ and $B = g^q \bmod P$;

B! cont

(d) receive from said other computing entity a random number $h \in Z_n^*$ such that $\left(\frac{h}{n}\right) = -1$;

e) check that $\left(\frac{h}{n}\right) = -1$ and, if so, select two random numbers u and v such that $\ell(u) = \ell((p - 1)/2)$, $\ell(v) = \ell((q - 1)/2)$ and provide to said other computing entity the values of $U = g^{2u}$, $V = g^{2v}$, $H_U = B^{(h^u \bmod n)}$, $H_V = A^{(h^v \bmod n)}$ and $H_{UV} = h^u h^v \pmod{n}$;

f) receive from said other computing entity a request to provide to said other computing entity values r and s, which said other computing entity randomly specifies should be either:

(1) $r = u$ and $s = v$; or

(2) $r = u + (p - 1)/2$, $s = v + (q - 1)/2$

g) provide the requested values r and s to said other computing entity.